

SUB
A17

A system and method for cryptographic communication among multiple users and a central service provider using in situ generated cryptographic keys. Each user communicates with the central service provider preferably using a user communication interface that includes an in situ key generator, which, after initialization with the user's own individual seed value, generates a unique cryptographic key. By distributing different user individual seeds unique to each user, each user's in situ key generator generates a unique set of keys. The central service provider also possesses an in situ key generator, and also preferably possesses a copy of all the individual seeds assigned to authorized users. The central service provider preferably communicates in a secure encrypted fashion with each user using cryptographic keys generated from that user's individual keys.